考虑成本时拓扑可调无标度网络鲁棒性研究 *

王尔申 [a,b]，王玉伟 [a]

(沈阳航空航天大学 a. 电子信息工程学院; b. 辽宁省通用航空重点实验室, 沈阳 110136)

摘　要：为了研究无标度网络拓扑结构对网络鲁棒性的影响，结合对复杂网络鲁棒性有重要影响的节点介数和边权重两种指标，提出一种考虑成本的拓扑可调无标度网络攻击方法。该方法在攻击网络中节点（边）时引入了节点（边）的攻击成本因素，以节点介数（边权重）来近似衡量节点（边）的攻击成本，采用不同节点（边）攻击策略对网络进行攻击，并采用最大连通子图相对值作为网络鲁棒性测度指标，利用该方法对无标度网络的幂率指数、平均度与网络鲁棒性的关系分别进行了研究。结果表明，采用蓄意攻击策略时，对于同一节点（边）攻击成本，无标度网络的幂率指数越小或平均度越大，网络的鲁棒性越强。仿真实验验证了该方法的有效性与可行性。

关键词：无标度网络；幂率指数；平均度；攻击策略；攻击成本；鲁棒性

中图分类号：TP393.02　　doi: 10.3969/j.issn.1001-3695.2017.08.0723

Research on robustness of tunable scale-free networks with cost

Wang Ershen[a, b], Wang Yuwei[a]

(*a. School of Electronic & Information Engineering*, *b. Liaoning General Aviation Key Laboratory*, *Shenyang Aerospace University*, *Shenyang* 110136, *China*)

Abstract: In order to investigate the effects of scale-free network's topology features on network robustness. Combining two indexes of node's betweenness and edge's weight, which has important influence on network robustness. This paper proposed a tunable scale-free network attack method with cost. This method considered the attack cost of nodes(edges) when the network was attacked. The method used the node's betweenness (edge's weight) to approximately measure the cost of nodes(edges) . This method used different attack strategies of nodes(edges) to attack the network. And this method used the largest component to quantify the network robustness. By using the method, this paper investigated the relation between scale-free network's power-law exponent, average degree and network robustness. When adopting the intentional attack strategy and fixing the cost value of nodes(edges) , the experimental results show that the lower the power-law exponent of scale-free networks or the higher the average degree of scale-free networks, the more robust of the network. The simulation results verify the effectiveness and feasibility of the proposed method.

Key Words: scale-free networks; power-law exponent; average degree; attack strategy; attack cost; robustness

0　引言

近年来，复杂网络受到越来越多学者的关注[1]。随着复杂网络研究的深入，其鲁棒性研究成为热点[2]。复杂网络鲁棒性是指网络受到攻击时，网络仍然能够继续维持其功能的能力[3]。

目前针对复杂网络鲁棒性方面的研究已取得许多重要进展。文献[4]以自然连通度为网络鲁棒性度量指标，研究了度分布对鲁棒性的影响，认为度分布越不均匀鲁棒性越强。文献[5]针对车载自组织网络的鲁棒性进行了分析，认为车载自组织网络对随机攻击有较强的鲁棒性，在蓄意攻击下显得比较脆弱，基于节点介数的蓄意攻击对网络的破坏更快、更强。在文献[6]中，作者针对不同的开放数据集和爬取的新浪微博数据集，通过计算移除部分节点后的巨片和连通子图数目等指标，着重分析了蓄意攻击对网络的影响。文献[7]分析了航空投递网络和陆运投递网络的鲁棒性，并对这两种网络的鲁棒性进行了优化。但是，这些研究并没有将节点（边）的攻击成本因素考虑在内。

从目前的研究进展来看，大部分关于复杂网络鲁棒性方面的研究并没有考虑到节点（边）的攻击成本因素[8-11]，文献[12]认识到这一问题，尝试在研究复杂网络鲁棒性时将节点的攻击成本考虑在内，采用节点的度来衡量节点的攻击成本。文献[12]

基金项目：国家自然科学基金资助项目（61571309，61101161）；辽宁省“百千万人才工程”资助项目；交通运输行业水上智能交通行业重点实验室开放课题；中央高校基本科研业务费（3132016317）资助项目；航空科学基金资助项目（2015ZC54010）；辽宁省教育厅资助项目（L2014059）

作者简介：王尔申（1980-），男，辽宁沈阳人，副教授，博士（后），主要研究方向为复杂网络、航空电子（wes2016@126.com）；王玉伟（1992-），男，河北邢台人，硕士研究生，主要研究方向为复杂网络鲁棒性．

认为当攻击成本较小时，节点度由小到大策略攻击效果较好；节点度由大到小策略只是在攻击成本较大时攻击效果最好，可见节点的攻击成本对节点攻击策略的攻击效果有一定的影响。然而，这些研究并没有以节点的介数来衡量节点的攻击成本，在攻击网络的边时也没有考虑边的攻击成本因素。

在前人研究复杂网络鲁棒性的基础上，文中首先介绍了一种基于成本的拓扑可调无标度网络攻击模型，然后研究了幂率指数和平均度对无标度网络鲁棒性的影响，最后给出文中得出的主要结论。

1　基于成本的拓扑可调无标度网络攻击模型

1.1　指数可调无标度网络

BA（barabasi albert）无标度网络度分布的幂率指数 γ 恒定为 3，而很多具有无标度特性的真实复杂网络的幂率指数在 2 到 3 之间。γ 越小，网络在度分布上的非均匀性越强；反之，度分布均匀性越强。文献[1]提出一种生成幂指数可调的无标度网络的算法。

1.2　介数

介数分为节点介数和边介数。介数能够反映节点（边）在整个网络中的影响力。节点介数具体定义为：

$$B_l = \sum_{j \neq l \neq i} \frac{\delta_{ji}(l)}{\delta_{ji}} \tag{1}$$

其中，$\delta_{ji}(l)$ 是连接节点 j 和节点 i 且经过节点 l 的最短路径数量，δ_{ji} 是连接节点 j 和节点 i 之间的最短路径条数。

1.3　加权复杂网络

现实中很多实际网络都是加权网络，Internet 中不同链路有不同的带宽和流量，航空网络中存在客流量的差异等，这些信息无法采用无权网络来描述，因此必须采用加权网络，为每条边赋予一定的权重来反映这些差异信息。加权网络可以用集合 $G=(N,W)$ 描述（N 为网络的节点数，W 为网络中边的权重），用加权邻接矩阵 $w=(w_{ij})_{n\times n}$ 来表示 $(i,j=1,2,.....N)$。边权与两个节点的度相关，假设边 e_{ij} 所连两个节点的度值分别为 k_i 和 k_j，文献[10]使用的权重模型定义为：

$$w_{ij} = (k_i * k_j)^{\theta} \tag{2}$$

其中，$\theta(\theta>0)$ 是一个可调的权重参数，用于描述网络边的异质度。

而文献[11]中给出了三种复杂网络边的赋权方式，分别为 $w_{ij}=B_{ij}$（边介数），$w_{ij}=(B_i * B_j)^{\theta}$（边两端节点介数乘积的幂指数形式）和 $w_{ij}=(k_i * k_j)^{\theta}$（边两端节点度乘积的幂指数形式）。

前人给出的复杂网络的一些加权方法，结合节点度和节点介数，文中采用复合边权重加权方法，其定义为：

$$w_{ij} = \alpha \frac{(k_i + k_j)}{\max\{k_i, k_j\}} + (1-\alpha)\frac{(B_i + B_j)}{\max\{B_i, B_j\}} \tag{3}$$

其中：α 为比重系数 $(0 \le \alpha \le 1)$。$\alpha = 0$ 代表边权仅节点介数相关，$\alpha = 1$ 代表边权仅节点度相关。式（3）中的加权方式可以利用参数 α 来灵活调节介数和度的比重。边权重综合考虑节点度和节点介数的影响，文中对于参数 α 取 0.5。

1.4　复杂网络鲁棒性测度

假如移除少量节点(边)后的网络中大多数节点仍然连通，就称该网络的连通性对节点（边）故障具有鲁棒性。复杂网络鲁棒性度量有很多种指标，如最大连通子图，平均反测地线距离等。文中采用最大连通子图相对值 G 来衡量复杂网络鲁棒性，最大连通子图相对值具体定义为 $G = N'/N$ [8]，N' 为网络受到攻击后的最大连通分支的节点个数，N 为网络受到攻击前节点总数。在某一攻击策略下，如果 G 的值越大，表明网络鲁棒性越强，即该攻击策略有效性越差。

1.5　攻击策略

1.5.1 节点攻击策略

文献[12]采用的三种节点度攻击策略分别为：节点度由小到大攻击（low degree removal strategy，LDRS）策略，节点度随机攻击（random degree removal strategy，RDRS）策略和节点度由大到小攻击（high degree removal strategy，HDRS）策略。

对上述文献中与节点度有关的概率移除方式进行改进可得到如下与节点介数有关的概率移除节点方式（节点移除后其所连的边也随之消失）：

$$p_i = \frac{B_i^{\beta}}{\sum_j B_j^{\beta}} \tag{4}$$

其中：$\beta < 0$ 对应节点介数由小到大攻击策略（Low Betweenness Removal Strategy，LBRS）：将网络中的节点按照其介数值由小到大排序后依次移除，$\beta = 0$ 对应节点介数随机攻击策略（Random Betweenness Removal Strategy，RBRS）：将网络中的节点按照其介数值随机选择后移除，$\beta > 0$ 对应节点介数由大到小攻击策略（High Betweenness Removal Strategy，HBRS）：将网络中的节点按照其介数值由大到小排序后依次移除。对于模型中参数 β 的选择，文中分别选取 $\beta = -3$，$\beta = 0$ 和 $\beta = 3$ 这三种情况来确定节点介数攻击策略。

1.5.2 边攻击策略

边攻击策略的定义是基于边的权重等重要性度量指标，即将边按照其权重的大小进行排序并移除。文中采用三种边攻击策略攻击网络，这三种边攻击策略定义分别如下：

a）边权随机攻击策略（random weight removal strategy，RWRS）。将网络的边按照边权重大小随机选择进行移除。

b）边权由小到大攻击策略（low weight removal strategy，LWRS）。将网络的边按照边权重由小到大的顺序进行排序，按照此排序结果对边进行移除。

c）边权由大到小攻击策略（high weight removal strategy，HWRS）。将网络的边按照边权重由大到小的顺序进行排序，按照此排序结果对边进行移除。

1.6　攻击成本

1.6.1 节点介数攻击成本

复杂网络的节点重要性指标有多种，如度，介数，接近度以及特征向量中心性等。文献[12]从“节点度”角度出发，以节点

的度来近似衡量节点的攻击成本，其中总节点度攻击成本定义为

$$\mu = \frac{\sum_{v \in Z} k_v}{\sum_{i=1}^{N} k_i} \tag{5}$$

其中：k_i 是节点 i 的度，N 是初始网络中的总节点数，k_v 是被移除节点的度，Z 是移除节点的数量总和。

考虑到节点介数也是节点重要性的度量指标，与文献[12]研究思路相似，本文则从“节点介数”的角度出发，以节点的介数来近似衡量节点的攻击成本，并假设攻击成本与节点介数成正比。总的节点介数攻击成本定义为

$$\rho = \frac{\sum_{v \in Z} B_v}{\sum_{i=1}^{N} B_i} \tag{6}$$

其中: B_i 是节点 i 的介数，N 是初始网络的节点总数，B_v 是被移除节点的介数，Z 是移除节点的数量总和。

1.6.2 边攻击成本

以往的研究往往忽略边的攻击成本因素，而复杂网络边的攻击成本并不一定相同。为研究边攻击成本对各种边攻击策略攻击效果的影响，本文采用边的权重来衡量复杂网络边的攻击成本，即 $\cos t_i = w_i$。总的边攻击成本定义为

$$\lambda = \frac{\sum_{l \in Z} w_l}{\sum_{i=0}^{M} w_i} \tag{7}$$

其中: w_i 是网络中边 i 的权重；M 是网络的总边数；Z 是移除网络边的数量总和。

1.7　算法流程

根据 1.1~1.6 节中的相关定义，基于介数（边）成本的复杂网络节点（边）攻击模型算法具体步骤设计如下：

a)按照 1.1 节中的算法生成一定规模指数可调的无标度网络。

b)按照式（1）求出网络中各个节点的介数；如果是边攻击则按照式（3）求节点之间所连边的权重。

c)按照式（4）的概率将网络的节点进行移除；如果是边攻击则按照 1.5.2 节中的边攻击策略进行复杂网络边的攻击。

d)设定复杂网络节点初始成本值，将被移除的节点的介数添加到 $\sum_{v \in Z} B_v$ 中，按照式（6）重新计算 ρ 值。如果 ρ 的值比所给成本值小，那么这个节点就被移除，重复步骤 c)d)直到 ρ 的值达到所给节点成本值；如果是边攻击则设定复杂网络边成本初始值，将被攻击的边的权重按照式（7）计算 λ 值，如果 λ 的值比所给成本值小，那么这条边被移除，重复此步骤直到 λ 的值达到所给的边成本值。

e)计算网络最大连通子图的相对大小 G。

2　仿真验证与分析

此部分将在考虑成本因素时，分别研究幂率指数和平均度对拓扑可调无标度网络鲁棒性的影响。每组实验均独立进行 40 次，通过取平均值得出最后仿真结果。

2.1　幂率指数对拓扑可调无标度网络鲁棒性的影响

为探讨幂率指数对网络鲁棒性的影响，采用前面所述的拓扑可调无标度网络的生成机制，生成节点数 $N=1000$，平均度 $<k>\approx 10$ 的无标度网络，选取不同的幂率指数分别进行实验。采用节点度攻击策略时幂率指数对网络鲁棒性的影响，如图 1 所示。采用节点介数攻击策略时幂率指数对网络鲁棒性的影响，如图 2 所示。采用边攻击策略时幂率指数对网络鲁棒性的影响，如图 3 所示。

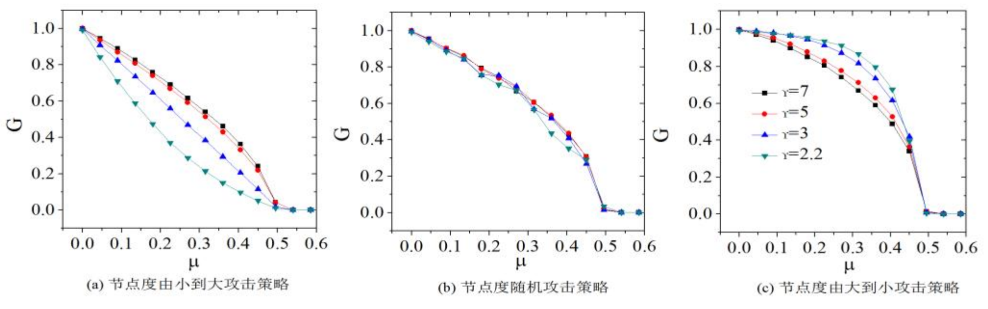


图 1　采用节点度攻击策略时幂率指数对网络鲁棒性的影响

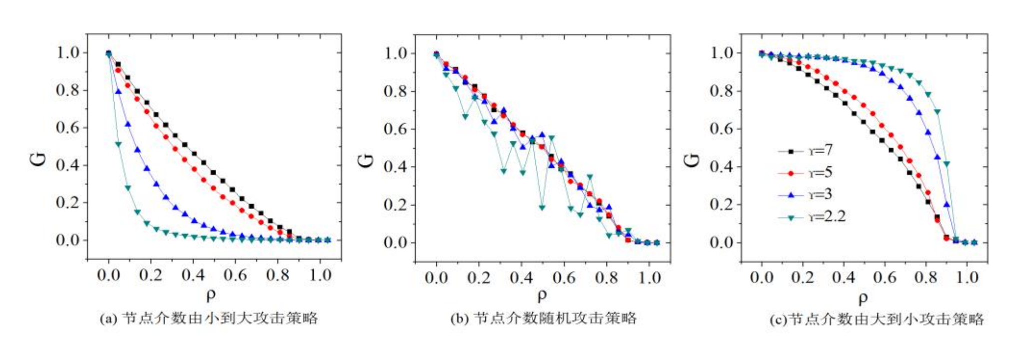


图 2　采用节点介数攻击策略时幂率指数对网络鲁棒性的影响

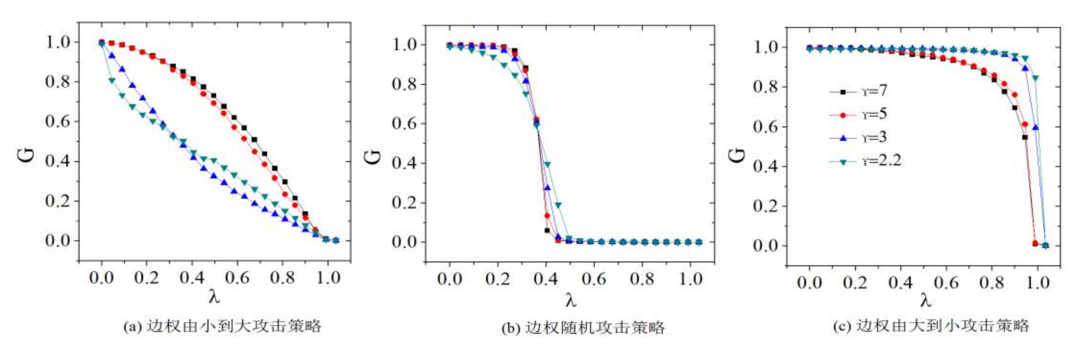


图 3 采用边攻击策略时幂率指数对网络鲁棒性的影响

图 1 为采用不同节点度攻击策略时幂率指数对网络鲁棒性的影响曲线。由图 1（a）得知，采用 LDRS 策略时，幂指数 γ 越小，网络鲁棒性曲线越陡，即网络鲁棒性越差。由图 1（b）得知，采用 RDRS 策略时，不同 γ 值对网络鲁棒性影响几乎相同。由图 1（c）得知，采用 HDRS 策略时，幂指数 γ 越小，网络鲁棒性曲线下降趋势越慢，即对应的网络鲁棒性越强。

图 2 为采用不同节点介数攻击策略时幂率指数对网络鲁棒性的影响曲线。图 2（a）中采用 LBRS 策略，幂指数 γ 越小，网络鲁棒性越差。图 2（b）中采用 RBRS 策略，幂指数 $\gamma=2.2$ 比 γ 取其他值时对应的网络鲁棒性曲线变化趋势较大，但整体趋势大致相同。图 2（c）中采用 HBRS 策略，幂指数 γ 越小，对应的网络鲁棒性越强。

图 3 为采用不同边攻击策略时幂率指数对网络鲁棒性的影响曲线。图 3（a）中采用 LWRS 策略，当 $0<\lambda<0.3$ 时，幂指数 γ 越小，网络鲁棒性越差；当 $0.3<\lambda<1$ 时，对于同一边攻击成本值，幂指数 $\gamma=3$ 时对应的网络鲁棒性最弱。图 3（b）采用 RWRS 策略，当 $0<\lambda<0.38$ 时，幂指数 γ 越大，网络鲁棒性越强；当 $0.38<\lambda<0.55$ 时，幂指数 γ 越小，网络鲁棒性越强；当 $0.55<\lambda<1$ 时，不同 γ 值下得到的网络鲁棒性曲线几乎重合，即采用 RWRS 策略且攻击成本较大时，不同 γ 值对网络鲁棒性影响几乎相同。图 3（c）采用 HWRS 策略，幂指数 γ 越小，对应的网络鲁棒性越强。

2.2 平均度对拓扑可调无标度网络鲁棒性的影响

为研究平均度对指数可调无标度网络鲁棒性的影响，当幂指数 γ 取 3 时，无标度网络的平均度<k>分别取不同值。采用节点度攻击策略时平均度对拓扑可调无标度网络鲁棒性的影响，如图 4 所示。采用节点介数攻击策略时平均度对拓扑可调无标度网络鲁棒性的影响，如图 5 所示。采用边攻击策略时平均度对拓扑可调无标度网络鲁棒性的影响，如图 6 所示。

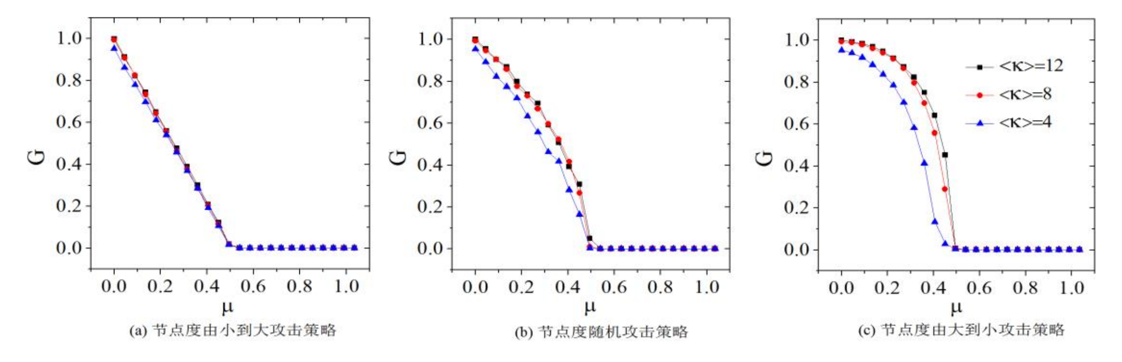


图 4 采用节点度攻击策略时平均度对网络鲁棒性的影响

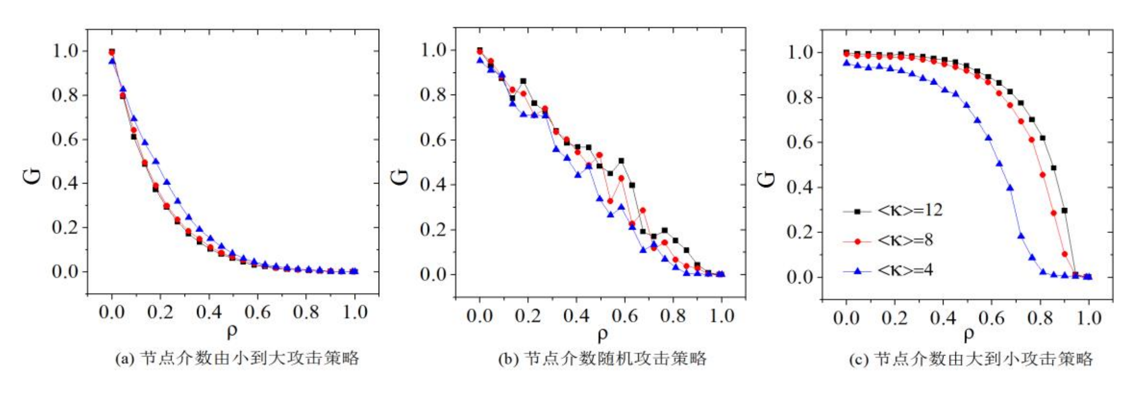


图 5 采用节点介数攻击策略时平均度对网络鲁棒性的影响

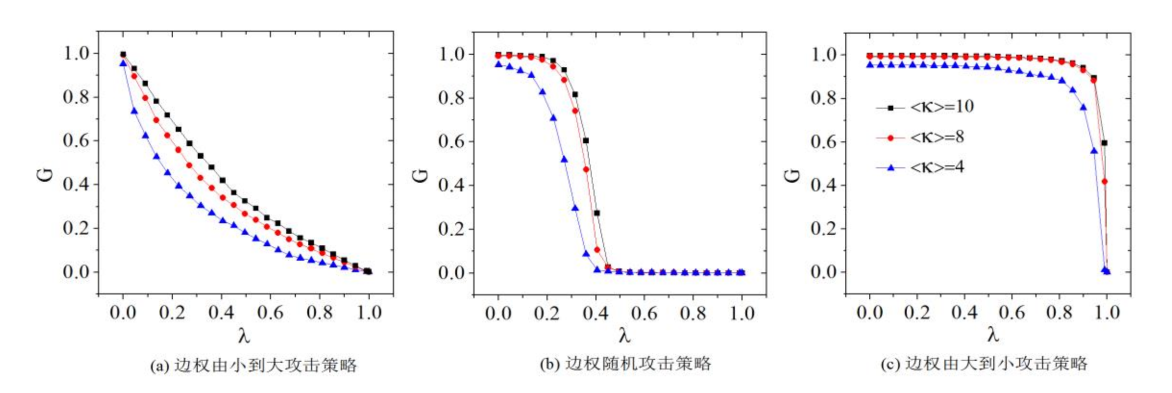


图 6　采用边攻击策略时平均度对网络鲁棒性的影响

图 4 为采用节点度攻击策略时平均度对拓扑可调无标度网络鲁棒性的影响曲线。图 4（a）中采用 LDRS 策略，不同平均度下得到的网络性能曲线几乎重合，这表明采用 LDRS 策略时，平均度的不同取值对网络鲁棒性影响几乎相同。图 4（b）中采用 RDRS 策略，当 $0<\mu<0.5$ 时，平均度越小，对应的网络鲁棒性越弱；当 $0.5<\mu<1$ 时，平均度的不同取值对网络鲁棒性影响几乎相同。图 4（c）中采用 HDRS 策略，当 $0<\mu<0.5$ 时，平均度越大，对应的网络鲁棒性越强；当 $0.5<\mu<1$ 时，平均度的不同取值对网络鲁棒性影响几乎相同。

图 5 为采用节点介数攻击策略时平均度对拓扑可调无标度网络鲁棒性的影响曲线。图 5（a）中采用 LBRS 策略，平均度越小对应的网络鲁棒性越强；图 5（b）中采用 RBRS 策略，平均度越小对应的网络鲁棒性越弱；图 5（c）中采用 HBRS 策略，平均度越大对应的网络鲁棒性越强。

图 6 为采用边攻击策略时平均度对拓扑可调无标度网络鲁棒性的影响曲线。图 6（a）中采用 LWRS 策略，平均度越大对应的网络鲁棒性越弱；图 6（b）中采用 RWRS 策略，当 $0<\lambda<0.5$ 时，平均度越大对应的网络鲁棒性越强；当 $0.5<\lambda<1$ 时，平均度的不同取值对网络鲁棒性影响几乎相同。图 6（c）中采用 HWRS 策略，平均度越小对应的网络鲁棒性越弱。

3　结束语

本文在前人研究复杂网络鲁棒性的基础上考虑了节点和边的攻击成本因素，将幂率指数和平均度对拓扑可调无标度网络鲁棒性的影响进行了研究。研究表明，当攻击成本不可忽略并采用蓄意攻击策略情况下（如文中采用的的 HDRS 策略，HBRS 策略或 HWRS 策略），节点或边的攻击成本值固定时，无标度网络的幂指数越小（度分布越不均匀）或平均度越大（网络越稠密），网络鲁棒性越强，网络越不容易被破坏。

参考文献：

[1] Goh K I, Kahng B, Kim D. Universal behavior of load distribution in scale free networks [J]. Physical Review Letters, 2001, 87 (27): 278701.

[2] Hong Chen, He Ning, Lordan O, et al. Efficient calculation of the robustness measure R for complex networks [J]. Physica A: Statistical Mechanics and its Applications, 2017, 478: 63-68.

[3] Nie Tingyuan, Guo Zheng, Zhao Kun, et al. New attack strategies for complex networks [J]. Physica A: Statistical Mechanics and its Applications, 2015, 424: 248-253.

[4] 吴俊，谭索怡，谭跃进，等. 基于自然连通度的复杂网络鲁棒性分析 [J]. 复杂系统与复杂性科学, 2014, 11 (1): 77-86.

[5] 冯慧芳，李彩虹. 基于复杂网络的车载自组织网络鲁棒性分析 [J]. 计算机应用, 2016, 36 (7): 1789-1792, 1806.

[6] 陆靖桥，傅秀芬，蒙在桥. 复杂网络的鲁棒性与中心性指标的研究 [J]. 计算机应用与软件, 2016, 33 (4): 302-309.

[7] 谢逢洁，崔文田. 加权快递网络鲁棒性分析及优化 [J]. 系统工程理论与实践, 2016, 36 (9): 2391-2399.

[8] Motter A E, Lai Y C. Cascade-based attacks on complex networks [J]. Physical Review E: Statistical Nonlinear and Soft Matter Physics, 2002, 66 (6): 065102.

[9] 彭兴钊，姚宏，张志浩，等. 基于节点蓄意攻击的无标度网络级联抗毁性研究 [J]. 系统工程与电子技术, 2013, 35 (9): 1974-1978.

[10] Wang Wenxu, Chen Guanrong. Universal robustness characteristic of weighted networks against cascading failure [J]. Physical Review E: Statistical Nonlinear and Soft Matter Physics, 2008, 77 (2): 026101.

[11] Mirzasoleiman B, Babaei M, Jalili M, et al. Cascaded failures in weighted networks [J]. Physical Review E: Statistical Nonlinear and Soft Matter Physics, 2011, 84 (2): 046114.

[12] Hong Chen, Cao Xianbin, Du Wenbo, et al. The effect of attack cost on network robustness [J]. Physica Scripta, 2013, 87 (5): 458-465.